International Journal of Computers and Informatics

Journal Homepage: https://www.ijci.zu.edu.eg

Int. j. Comp. Info. Vol. 11 (2026) 36–58

Paper Type: Review Article

Image Spoofing in Biometrics: Evolving Threats, Detection Strategies, and Future Directions

Islam Mohamed [1], Ahmad Salah [1,2,*], Marwa Abdellah [1], and Amr M. Abdelatif [1]

[1] Department of Computer Science, Faculty of Computer and Informatics, Zagazig University, Zagazig, Egypt;
[2] Department of Computing and Information Sciences, College of Computing and Information Sciences, University of Technology and Applied Sciences, Ibri, Al Dhahirah, Sultanate of Oman;
Emails: eng.eslam.fci2017@gmail.com, ahmad.salah@utas.edu.om, marwaabdella2@gmail.com, amro43210@gmail.com.

Received: 13 Jan 2026 **Revised**: 17 Apr 2026 **Accepted**: 25 Jun 2026 **Published**: 27 Jun 2026

Abstract

Over the past few decades, biometric technology has advanced significantly, beginning with the earliest studies on voice and facial recognition and continuing to this day with a variety of highly accurate systems. These modalities range from widely deployed ones like fingerprint, face, or iris to less common modalities like handwriting or signatures. Image spoofing poses a significant threat to security systems that rely on visual data for authentication. This survey evaluates a number of the most widely used strategies in each field, looking at how they work, their advantages, and any potential drawbacks. We will wrap up by summarizing the current state of the art, highlighting the unresolved issues, and providing an overview of potential future paths for this study. Additionally, we will present an organized future research roadmap, and identify unresolved obstacles. This survey makes three distinctive contributions: (i) a unified cross-modal taxonomy classifying attacks by type, modality, and detection strategy; (ii) a critical analysis of cross-domain generalization gaps, explaining why certain detection approaches outperform others across datasets; and (iii) integrated coverage of emerging generative-AI threats including GAN-based and diffusion-model-generated spoofs alongside practical deployment considerations such as computational cost and edge-device suitability.

Keywords: Presentation Attack Detection; Liveness Detection; Biometric Security; Deep Learning; Anti-Spoofing; Convolutional Neural Networks; GAN-based Attacks.

1 | Introduction

With the advent of biometric technology, the majority of organizations have switched from traditional methods. A biometric recognition system's objective is to identify or confirm a person's identity based on behavioral and/or biological traits. Voice mail, building and critical infrastructure access control, computer or mobile device log-in, criminal identification, airport check-in, and transaction authentication are examples of applications. Biometrics range from traditional fingerprint, iris, face, and voice recognition to developing modalities including gait, hand-grip, ear, and electroencephalograms. Each modality has unique strengths and weaknesses [1]. We divide spoofing into four categories: biometric spoofing, text message

Corresponding Author: ahmad.salah@utas.edu.om

and Caller ID spoofing, network spoofing, and sensor spoofing. However, the major focus of this survey rests in the field of image spoofing, which includes

Face Spoofing: Face recognition is widely utilized for both personal and business purposes, including accessing laptops, computers, ATMs, online banking, airports, and border control [2, 3]. Although biometric approaches are more accurate, they might also be more vulnerable. The printing attack [4, 5], video replay attack [6], and 3D mask attack [7] are the most common spoofing techniques. In 2005, K. Kollreider introduced the first liveness approach based on the structural tensor of facial images [8]. The increasing use of facial recognition systems has also given rise to new concerns, namely about the system's vulnerability and the data collecting subsystems [9]. Spoofing is no longer limited to fantastical Hollywood films. A real-life incident was recently reported in which a young individual from Hong Kong boarded a plane to Canada wearing a flat hat and disguising himself as an elderly man. This individual successfully eluded border control agents by donning a silicone face and neck mask. There are certain distinctions between genuine and fake faces, and they are mostly seen in the texture, motion, and depth information of the images. Using these distinctions, we can develop robust anti-spoofing systems to distinguish between real and fake faces. Recent research on face anti-spoofing detection has shown significant results.

Fingerprint Spoofing: Since the late nineteenth century fingerprint recognition technology has been employed as an identifier due to the belief that all individuals have a unique fingerprint. The use of fingerprints for this purpose was first suggested in [10]. As indicated, many subsequent studies also supported this notion; see some examples here [11, 12]. As such, fingerprints remain the most popular biometric modalities currently in use today (due to their uniqueness and the relatively inexpensive cost of sensors) and therefore it is likely that many will be targeted by potential impersonators who can create artificial fingerprints from common materials (such as silicone, gelatin or Play-Doh). Attackers may be able to fraudulently obtain the same access rights as legitimate users even if they are not listed as a valid user; this includes when they have successfully registered with the system.

Iris Spoofing: The iris can provide a lot of textural data for biometric identity verification [13]. The uniqueness of this biometric technology also makes it very reliable; however false acceptance or rejection will occur with a higher frequency if an attacker uses one or more of the many possible iris spoofing attack techniques. Currently, Daugman's first successful algorithm, called IrisCodes [14], has been adopted by multiple commercial and national biometric deployments globally.

This article provides an inclusive cross-modal study comparing image spoofing detection methods, as opposed to past survey articles that have been limited to studying one or two modalities. In this article, a systematic review of more than 68 peer-reviewed articles is completed from 2010-2026. The detection methods are categorized by their technology, as well as identifying challenges specific to each type of modality and exploring those critical challenges.

Unique Contributions of This Survey: Unlike prior surveys that concentrate on a single modality, this work introduces a unified cross-modal taxonomy, analyzes cross-domain generalization issues in depth, and addresses the rising threat of generative-AI spoofing alongside practical deployment metrics. These contributions place this survey at a broader analytical scope than preceding reviews focused on individual modalities [15].

1.1 | Literature Search Methodology

Literature Selection Methodology: The literature included in this survey was identified through a systematic search of the Scopus, IEEE Xplore, Web of Science, and Google Scholar databases. Boolean search strings combined biometric modality keywords (face, fingerprint, iris) with anti-spoofing terminology (presentation attack detection, liveness detection, spoof detection, PAD). The search was restricted to peer-reviewed journal articles and conference proceedings published between 2010 and early 2026, yielding an initial pool of over 200 candidate papers. Articles were included if they (a) proposed or evaluated a concrete detection method for at least one biometric modality, and (b) reported results on a recognized benchmark or publicly described dataset. Review papers and meta-analyses were included for background context but excluded from the performance-comparison tables. Duplicate or substantially overlapping entries were consolidated, producing the final corpus of 68 primary studies reviewed here.

The rest of this document is structured as follows. Section 2 provides background material and a taxonomy of spoofing attacks. Section 3 reviews the related literature on face, fingerprint, and iris

spoofing detection, including open challenges and a summary table. Section 4 concludes the paper.

2 | Background

2.1 | Taxonomy of Image Spoofing Attacks

To provide a structured foundation for the review, Table 1 presents a three-dimensional taxonomy that classifies spoofing attacks according to (a) attack type, (b) target sensing modality, and (c) the primary category of detection strategy employed to counter them. At the attack-type dimension, attacks are grouped into 2D artifact attacks (printed photographs, video-replay), 3D physical attacks (silicone masks, 3D-printed structures), and digital synthesis attacks (GAN-generated images, deepfakes, diffusion-model outputs). At the modality dimension, each attack is mapped to the face, fingerprint, or iris recognition subsystem it targets. At the detection-strategy dimension, countermeasures are categorised as texture/feature-based, deep learning-based, multi-modal fusion-based, or domain-generalisation-based. This taxonomic view reveals a clear pattern: texture-based and CNN methods dominate face PAD research, whereas fingerprint and iris communities continue to rely more heavily on handcrafted features and limited publicly available data, partly due to the relatively smaller number of spoof acquisition databases in those modalities.

Table 1. Three-Dimensional Taxonomy of Image Spoofing Attacks

Attack Type	Target Modality	Detection Strategy	Example Methods
2D Artifact Attacks	Face, Fingerprint, Iris	Texture/Feature-based, CNN	LBP [24,33], Haralick texture [24], Gabor [47]
3D Physical Attacks	Face(primaril)	Deep Learning, Multi-modal Fusion	Deep Dictionary Learning [42], RGB-D Fusion [36], ART+ML [45]
Digital Synthesis (GAN/ Diffusion)	Face, Fingerprint, Iris	Domain Generalisation, Adversarial Learning	SpoofGAN [50], DDPM [51], StyleGAN [58], MFAE [22]
Contact Lens / Artificial Eye	Iris	Spectrographic, LFC, EVM	Daugman [55], Raghavendra [56], EVM [57], IensNet [59]
Artificial Finger (Silicone/Gelatin)	Fingerprint	Ridge/Valley Analysis, Transfer Learning	Tan & Ser [48], Dubey [47], TL-Efficient-SE [53], VGG16+ResNet [52]

PAD = Presentation Attack Detection (sensor-level detection of physical artefacts); Liveness Detection = a PAD sub-category focused on physiological signals (pulse, blink, pupil dilation); Biometric Forgery = post-capture digital manipulation of biometric samples. These distinctions are maintained consistently throughout the paper.

In computer science, biometrics refers to the automatic identification of persons using biological traits. Biometrics were first used over 4000 years ago by the Babylonian Empire to protect legal contracts against fraud and fabrication. Fingerprints were imprinted on the clay tablets where the contracts were inscribed. The widespread use of the Internet and mobile devices has led to a surge in biometric applications and research, opening up new areas. Biometric spoofing will never provide 100% efficiency since it is strongly reliant on device shortcomings. For example, the simplest way of spoofing a fingerprint, using tracing paper and duct tape, may only deceive low-quality fingerprint readers. Such vulnerabilities are commonly found in commercial entry-level

mobile devices. The same approach applies to tricking the face recognition technology. On low-end handsets, the latter detects your face by comparing it to one stored in the phone's memory. As a result, providing a natural-size photo may be sufficient to unlock the phone. Meanwhile, premium commercial smartphones typically utilize facial recognition algorithms based on a 3D scan of your face. It is nearly impossible to deceive this system without using drastic measures. However, the biometric system is open to malevolent assault by unauthorized users, posing a serious risk to the system's security functionality. As a result, creating an anti-spoofing system with great durability, quick response times, and high detection accuracy is crucial. There are four main categories of spoofing: biometric spoofing, text message and Caller ID spoofing, network spoofing and sensor spoofing (see Figure 1 for a broader overview), but this survey will concentrate on image spoofing.

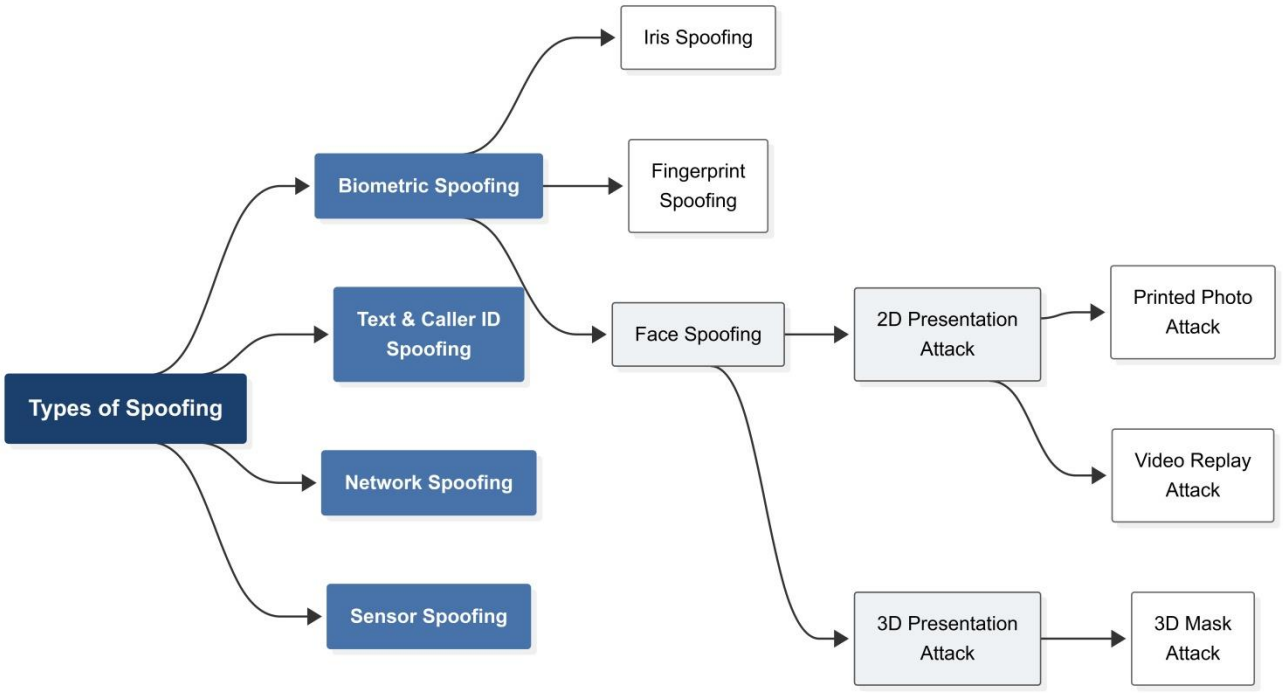

Figure 1. Categories of Spoofing.

According to the application, 1) Verification (or authentication) and 2) Identification are the two main modes in which biometric systems usually operate. A system for authentication seeks to verify or refute a stated identity (one-to-one matching), whereas a system for identification seeks to identify a particular person (one-to-many matching). The feature-to-reference comparison process, which underlies both modes despite certain distinctions, is essentially the same and involves the processes shown in Figure 2.

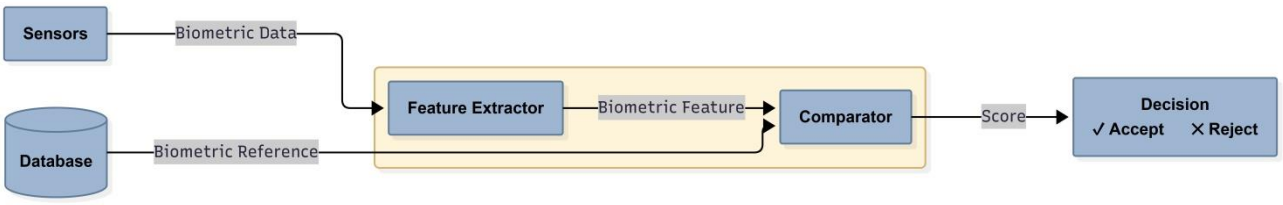

Figure 2. The feature-to-reference Comparison Process.

Initially, a sensor (such as a digital camera) is used to get a biometric sample (such as a facial image). After that,

biometric characteristics like face intensity, color, or texture are taken out of the sample. These might be a collection of parameters (or coefficients) that offer a more precise and pattern-recognition-friendly compact representation of the biometric sample. Biometric characteristics that discriminate between biometrics taken from different persons should reduce changes caused by acquisition or ambient variables (such as lighting, posture, and facial expression). The properties of a particular biometric sample are compared to one (for verification) or more (for identification) biometric references that were previously obtained during the enrollment phase in order to ascertain or confirm the identity corresponding to the sample. A comparator that generates a score indicating how comparable the characteristics and references are does these comparisons. In the case of verification, the conclusion is an affirmative or negative answer; in the case of identification, it is the name of the closest match.

2.2 Evaluation Metrics for Anti-Spoofing Systems

Image spoofing (presentation attack detection) systems often define the task as a binary classification problem, with genuine samples representing the positive class and spoofing attacks representing the negative class. These systems' performance is assessed using standardized metrics that quantify both classification errors, and threshold-dependent behavior.

2.2.1 Core PAD Metrics

As shown in Table 2, the ISO/IEC 30107-3 standard's major evaluation criteria are extensively used in the literature. These metrics evaluate how well the system distinguishes between presentation attacks and genuine presentations.

Table 2. Core PAD Metrics (ISO/IEC 30107-3)

Metric	Full Name	Description
APCER	Attack Presentation Classification Error Rate	Proportion of attack samples misclassified as bona fide
BPCER	Bona Fide Presentation Classification Error Rate	Proportion of bona fide samples misclassified as attacks
ACER	Average Classification Error Rate	ACER = (APCER + BPCER) / 2

BPCER represents the extent to which an authorized user is incorrectly rejected by the system, whereas APCER represents the extent to which an unauthorized attacker can successfully trick the system. Both ACER and BPCER, which combine the two forms of mistakes, are frequently employed in research. When comparing models with different decision thresholds, they provide useful metrics. While EER is a popular statistic for determining the best operating point, AUC assesses a model's ability to distinguish between all presentations from two distinct classes (bona fide and presentation attack).

2.2.2 Threshold-Based Metrics

In addition to PAD-specific metrics, threshold-dependent metrics are typically used to provide more detailed information on system performance across different operating points. Table 3 summarizes these statistics.

Table 3. Threshold-Based Evaluation Metrics

Metric	Full Name	Description
EER	Equal Error Rate	The operating point at which false acceptance and false rejection rates are equal
HTER	Half Total Error Rate	The average of error rates at a predefined threshold
AUC	Area Under Curve	Represents the overall discriminative capability across all thresholds

These measures are especially useful when comparing various models in the absence of a preset decision criterion. AUC measures the overall separability of bona fide and presentation attack classes, whereas EER is often used to find the best operating point.

2.2.3 Evaluation Protocol

A validation set is commonly used to calculate a decision threshold, which is often based on the Equal Error Rate (EER) or a predetermined operational need. This threshold is used to determine the test set's key evaluation metrics APCER, BPCER, and ACER. Figure 3 depicts the whole evaluation process, which includes data splitting, threshold selection, classifier assessment, and performance measure calculation.

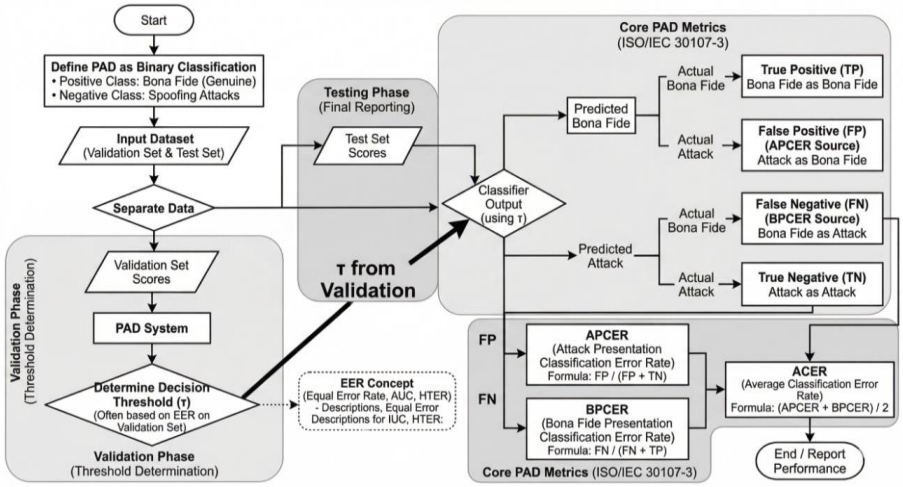

Figure 3. Evaluation pipeline for image spoofing detection, including threshold determination and computation of APCER, BPCER, and ACER.

The decision threshold is determined during the validation process and used to generate classification outputs during the testing phase, as illustrated in the image. APCER, BPCER, and ACER are then calculated by calculating the true positives, false positives, false negatives, and true negatives from these outputs.

2.3 Benchmark Datasets

In image spoofing studies, standardized benchmark datasets are essential for reproducible assessment. The most popular public datasets for each of the three modalities included in this survey are shown in Table 4. To show cross-dataset generalizability, researchers are urged to present results from several datasets.

Table 4. Key benchmark datasets used in image spoofing detection research.

Dataset	Modality	Year	Subjects	Attack Types	Approx. Samples
NUAA	Face	2010	15	Photo (printed)	12,614
Replay-Attack	Face	2012	50	Print, video replay	~1,300 videos
CASIA-FASD	Face	2012	50	Print, video, warped photo	~600 videos
MSU-MFSD	Face	2015	35	Print, video replay	~280 videos
3DMAD	Face	2013	17	3D mask (ThatsMyFace)	255 videos
SMAD	Face	2017	65	Silicone mask	130 videos
LivDet 2011-2023	Fingerprint	2011+	Varies	Silicone, gelatin, play-doh, latex, wood glue	Varies by year
FVC2004	Fingerprint	2004	100	Synthetic / artificial fingers	800 images
ATVS-FIr DB	Iris	2013	50	Print attack, video replay	~800 sequences
LivDet-Iris 2020	Iris	2020	Varies	Textured contacts, print, synthetic	4,000
Warsaw Post-Mortem	Iris	2015	Varies	Cadaver / post-mortem iris	Varies

Table 4 highlights well-established benchmarks, though each carries notable limitations. CASIA-FASD and Replay-Attack (both 2012) lack modern high-resolution video, sensor diversity, and GAN-generated or deepfake attack samples, limiting relevance to current threat models. 3DMAD relies on a single silicone mask manufacturer, artificially restricting material diversity. LivDet fingerprint datasets cover a limited range of fabrication materials and optical sensors, making cross-sensor generalisation difficult to assess. Future benchmark development should incorporate diverse sensors, generative-AI-based attack types, and standardised

cross-dataset evaluation splits to better reflect operational conditions.

3 | Related Works

This section reviews three primary categories of image spoofing attacks. Face spoofing is examined first as the most extensively studied modality, followed by fingerprint spoofing and iris spoofing.

Face spoofing: Biometric researchers in academia and business are increasingly focused on detecting presentation attacks in face recognition systems. There is much work on the vulnerability of data capturing subsystems and detection mechanisms for presentation attacks in facial recognition systems [16, 17]. There are two ways to spoof faces: 2D spoofing and 3D spoofing. Both types can be further classified into different attacks such as photo attacks, video attacks, and 3D mask attacks [18, 19]. These days, 3D masks are easily available in the market, and all these attacks are used in face modality [20, 21]. Photos and videos are easily available due to internet social sites, and videos can be taken from mobile devices or any other digital device.

2D spoofing: An attacker can use an image attack, which falls under the category of 2D spoof, to gain access to a system via a biometric modality such a laptop, tablet, or mobile phone screen. This image may have been taken using a digital camera, or it might have been downloaded from Facebook, Instagram, or Twitter [22]. To trick the facial recognition system, the attacker only has to print out the picture of the target or show it on a digital device. Because so many images of a certain individual are readily available online, attackers are now able to easily carry out photo attacks by using social media platforms to target face recognition biometric systems. He et al [23] proposed deep Parametric Rectified Linear Units (PReLU) for improved CNN training**.** This study focused on neural networks for image classification. Image categorization may be performed in two methods.

The second technique utilized Parametric Rectified Linear Unit (PReLU). PReLU improves layout matching. Agarwal et al [24] suggested a method for identifying face parodies based on surface highlights. Haralick identifies RDWT sub-groups as a savvy and direct opponent of mocking calculation that focuses on squares. Patel et al. [25] suggested a method for detecting face spoofing using facial movement cues such as eye blinks and Deep Texture Features. This approach is used for two-dimensional attacks. This approach compares saved frames to pictures retained for authentication. This approach was tested on many public databases and produced positive results. Sepas-Moghaddam et al. [26] suggested a face spoof detection approach using a light field imaging framework. Rather than relying solely on local binary patterns, this approach exploits the color and texture variations associated with the different directions of light captured by light field cameras. The framework was tested on the IST Lenslet Light Field Face Spoofing Database (IST LLFFSD) and produced highly effective results against multiple presentation attack types. Wang et al [27] provide a new consistency regularization strategy for deep face anti-spoofing that works well in both full-supervised and semi-supervised tasks. Solomon et al [28] Present FASS, a new face anti-spoofing system that combines the findings of two classifiers. The random forest algorithm combines seven no-reference image quality parameters from face photos with a deep learning classifier that utilizes the full image as input. To capture the high-precision hyperspectral information of the detected face, Shijie et al [29] design a snapshot hyperspectral image sensor based on metasurface nanostructures. The authors subsequently utilized their novel sensor to construct a workable anti-spoofing face recognition system. In order to

specifically estimate the spoof-related patterns for face anti-spoofing, Liu et al [30] provide a unique adversarial learning approach. Spoof faces are separated into fake traces and their real counterparts in two stages the additive phase and the inpainting step drawn from the physical process. This two-step modeling method has the potential to significantly minimize the search space for adversarial learning of spoof trace. In order to successfully address long-tail spoof types, reversely constructing new spoof faces from the disentangled spoof traces may be done using trace modeling. In order to provide domain separability, Sun et al. [31] align each domain's live-to-spoof transition (i.e., trajectory) to be the same, as opposed to creating a domain-invariant feature space. The Face Anti-spoofing strategy of separability and alignment (SA-FAS) is formulated as an invariant risk minimization (IRM) issue. The objective is to develop a domain-invariant classifier that is domain-variant in feature representation. Wang's proposal [32] is to utilize a single model for face forgery detection that can identify both temporal and spatial artifacts. The researchers discovered, however, that existing methods might rely heavily on one type of artifact while overlooking others. To overcome this limitation, they introduced a unique training technique dubbed AltFreezing for more generalized video face forgery detection. The goal of AltFreezing is to make the model more capable of identifying temporal as well as spatial errors. Liu et al [17] use large-scale VLMs such as CLIP and uses the textual feature to dynamically modify the classifier's weights in order to explore visual characteristics that are generalizable. Turhal et al [33] concatenate multi-level LBP features taken from device-dependent data. FPA (face presentation attack) may be detected using device-independent color spaces, regardless of attack type or device utilized. Asmitha et al [34] assess face recognition performance by combining RetinaFace and I-AF algorithms. The suggested technique, which prioritizes Extended Euclidean length above feature embedding normalization, significantly improves accuracy when compared to other methodologies like Viola-Jones, AlexNet, and Tiny YOLO3. Sabri et al [35] combine the characteristics of two strong deep learning architectures, DenseNet201 and MiniVGG, which were carefully selected based on a detailed comparison research of DenseNet201, DenseNet169, VGG16, MiniVGG, and ResNet50. In recent years, innovation in face anti-spoofing has focused on cross-domain generalisation and novel texture patterns. Kim and Kwon [36] developed a cross-domain system combining RGB-D fusion with domain adversarial training, achieving competitive accuracy across multiple benchmarks. Li et al. [37] proposed an Enhanced Channel Attention mechanism with an Intra-Class Differentiator (ECA+ICD) to better separate overlapping live and spoof feature distributions. El-Rashidy et al. [38] introduced the Comprehensive Correlational Pattern (CCP) texture descriptor paired with MTCNN, outperforming conventional LBP-based methods on several standard benchmarks.

3D spoofing: The 3-D mask assault differs from video and picture attacks by incorporating depth into face characteristics. In a 3D mask assault, attackers create a 3D mask of the impersonator, making it challenging to develop defenses against spoofing [39]. These assaults are less common compared to other types [40]. 3D masks may be manufactured of many materials and sizes, including paper, plastic, and silicon. In response to the rising threat of 3D image spoofing, researchers are actively developing detection

techniques. Feng et al. [41] improved 2D and 3D spoofing detection by combining picture quality cues (Shearlet) and motion cues (dense optical flow) with a hierarchical neural network. Manjani et al. [42] established a difficult silicon face mask database (SMAD) and a PAD approach employing multilevel deep dictionary learning to address 3D mask spoofing in various situations. Menotti et al. [43] compared two deep representation approaches for detecting spoofing across biometric modalities. One approach involves optimizing network architectures' hyperparameters (AO), while another focuses on learning filter weights using back-propagation (FO). Lucena et al. [44] introduced FAS-Net, a face PAD network that detects picture, video, and mask threats. The model used transfer learning using a pre-trained VGG-16 model architecture, with the exception of the top layers. Hamdan et al. [45] integrated the mask PAD approach with a facial recognition system. The researchers employed Angular Radial Transformation (ART) to extract shape information from RGB pictures, which were then fed into a Maximum Likelihood (ML) classifier. A new attack vector against 3D face authentication systems is discovered by Wu et al. [46] when they investigate the security of 3D liveness detection systems that employ structured light depth cameras. The study presents DepthFake techniques capable of spoofing 3D face authentication systems using only a single 2D image.

Critical Analysis of Face Spoofing Detection: While face presentation attack detection is the most extensively researched biometric modality, it continues to face significant operational hurdles. Deep learning architectures, particularly CNNs, achieve near-perfect accuracy on intra-dataset evaluations but frequently suffer steep performance drops in cross-domain scenarios involving unknown lighting conditions or novel spoofing materials. Furthermore, established benchmark datasets like CASIA-FASD and Replay-Attack lack the sensor diversity and high-resolution generative AI (deepfake) samples necessary to represent modern threat models. Future advancements must prioritize domain-generalization techniques and lightweight architectures capable of processing high-fidelity video streams on edge devices without prohibitive computational latency.

Fingerprint spoofing: Dubey et al. [47] introduced a new approach for detecting fingerprint liveness by merging low-level highlights from SURF, PHOG, and Gabor wavelet. A suggested unique score level integration module combines the results of two distinct classifiers. In order to avoid fingerprint sensor spoofing, Tan et al. [48] proposed a programming technique that combines ridge signal and valley noise analysis. The researchers experimented with a large dataset of real individuals, altering the substance and moisture levels in fake samples. The optical Identix scanner produced exceptional results with an Equal Error Rate of 0.9%. Similarly, Marasco et al. [15] investigated fingerprint recognition systems and identified vulnerabilities that can lead to impersonation attempts. Artificial fingers made of play-doh, silicone, and gelatin are a potential risk. Almajmaie et al [49] developed a new technique for fingerprint recognition based on associative memory. The experiments were carried on databases like FVC (2004), international NIST databases and an internal database. In order to improve the performance of fingerprint PAD algorithms beyond what can be achieved through training on a small number of publicly available "real" datasets, Grosz et al [50] aim to demonstrate the utility of synthetic (both bona fide and PA style) fingerprints. Tang et al [51] provide a method for creating high-quality patch size fingerprint photographs while preserving their distinctive and complicated properties. The authors employed a novel combination of a generative adversarial network (WGAN-GP) and a Denoising Diffusion Probabilistic Model (DDPM) to achieve their synthesis objectives. To merge global fingerprint structures with localized features from many patches, they employ style transfer techniques using a cycle autoencoder network (cycleWGAN-GP). Deep learning ensembles and transfer learning have also been developed for fingerprint spoof detection. Cheniti et al. [52] used a dual-stream architecture that combined pre-trained VGG16 and ResNet50 models to obtain an Average Classification Error (ACE) of 0.28% on the LivDet 2013 dataset. Pallakonda et al. [53] presented TL-Efficient-SE, a model combining EfficientNetB0 with a Squeeze-and-Excitation (SE) attention mechanism via transfer learning to

address cross-sensor generalisation.

Critical Analysis of Fingerprint Spoofing Detection: Despite representing the oldest deployed biometric modality, fingerprint PAD research exhibits a notable asymmetry relative to face anti-spoofing in three respects. First, the public corpus is substantially smaller: the LivDet series remains the dominant evaluation platform, and cross-sensor generalisation—tested, for instance, in [53] is still an unsolved problem because different optical, capacitive, and thermal sensors produce markedly different ridge-valley representations. Second, whereas face PAD has benefited from large-scale annotated databases (e.g., CelebDF, FaceForensics++), equivalent resources for artificial-finger attacks across diverse fabrication materials (silicone, gelatin, ecoflex, wood glue) are scarce, limiting the statistical power of deep learning evaluations. Third, the ensemble and transfer-learning strategies recently applied to fingerprint PAD [52, 53] demonstrate promising accuracy, but the literature rarely reports inference latency or memory footprint, both of which are critical for deployment in embedded fingerprint readers with constrained processors. Future work should prioritise cross-material, cross-sensor evaluation protocols and report computational benchmarks alongside accuracy metrics to support fair comparison.

Iris spoofing: Although iris recognition is a very accurate biometric technology, it is a relatively new study topic compared to fingerprints or faces, with early investigations going back to the 1990s [54]. Iris spoofing has a brief history compared to other well-studied practices. Most iris spoofing assaults reported in the literature fall into one of three categories: picture attacks, contact-lens attacks, or artificial-eye attacks. Daugman, known as the "Father of Automatic Iris Recognition" for his pioneering contributions in the subject [55], proposed sensor-level anti-spoofing countermeasures for iris biometrics. According to Daugman method [55], the spectrographic features of ocular tissue (such as fat or blood) can serve as a liveness cue in iris detection. Spectrographic analysis can detect spoofing attacks whether the iris provided is a glass eye, image, or dead tissue. Raghavendra in [56] created a presentation assault detection approach using a Light Field Camera (LFC). The approach, based on a library of 104 distinct iris patterns, assesses focus variance across depth pictures created by the LFC. A method for detecting presentation attacks using Eulerian Video Magnification (EVM) is described in [57] for video-based iris recognition systems. Because this solution requires an iris video, it falls under sensor-level approaches, as traditional iris scanners only capture single pictures. The approach has proven effective even against video assaults. A conditional StyleGAN-based iris synthesis mode is presented by Bhuiyan [58], who makes a distinctive addition to the advancement of post-mortem iris identification research. Convolutional Neural Networks as well as Deep Learning Ensembles were also key factors in recent advancement of Iris Presentation Attack Detection. The authors Sharma and Selwal [59], proposed IensNet, a combination of three pre-trained, fine-tuned deep models (Resnet, DenseNet161 & VggNet), that were all optimized for their specific application in detecting reliable iris presentations attacks. Likewise, the authors Das et al. [60] found success with extracting deep features from a CNN applied to their own dataset of Bona Fide and Presentation Attacks of Iris Images. The researchers reported a high accuracy of 92.51%.

Critical Analysis of Iris Spoofing Detection: Iris PAD algorithms exhibit high reliability under controlled conditions, often leveraging unique physiological cues such as pupillary oscillation or the spectrographic properties of ocular tissue. However, this field is constrained by a severe lack of large-scale, publicly available datasets compared to face biometrics. The evaluation of advanced attacks, such as textured contact lenses, prosthetic eyes, or post-mortem presentations, relies heavily on custom or private databases, limiting the reproducibility and standardized benchmarking of new deep learning models. Addressing this data scarcity—potentially through high-quality synthetic generation techniques like conditional StyleGANs is a critical prerequisite for the continued evolution of iris spoofing detection.

3.1 Open Challenges and Future Directions

Even with significant advancements in image spoofing detection, a number of unresolved issues remain. Due to variations in illumination, sensor technology, and attack materials, models trained on one dataset often deteriorate on unknown domains, making cross-database generalization a crucial bottleneck. Although there is no comprehensive solution, domain-generalization techniques like frequency-domain autoencoders [22] and IRM-based alignment [31] are motivated by this domain-shift issue. A second issue is the arms race aspect of spoofing: as detection algorithms improve, adversaries create more sophisticated attacks, such as 3D-printed silicone masks [42], structured-light DepthFake vulnerabilities [46], and GAN-generated synthetic identities. To detect such threats, systems must be adaptable on a constant basis.

Cross-Domain Generalisation: A Critical Bottleneck: The gap between within-dataset and cross-dataset performance constitutes one of the most persistent challenges in biometric anti-spoofing. Models that achieve near-perfect accuracy on a held-out split of their training corpus frequently exhibit substantial degradation when evaluated on data collected with different sensors, lighting conditions, or spoof fabrication materials. For example, domain-adversarial training approaches such as [36] reduce but do not eliminate this gap, and IRM-based alignment [31] similarly requires careful domain partitioning during training that may not be feasible in operational settings. Several factors explain why cross-domain generalisation remains hard: (i) spoof traces are often low-level sensor artefacts rather than semantically meaningful cues, so they do not transfer across acquisition devices; (ii) publicly available datasets are too few and too small to sample the distribution of real-world attack scenarios; and (iii) the domain-shift problem is compounded by the arms-race nature of spoofing, where adversaries continuously adapt their materials to evade the latest detectors. Prospective solutions include meta-learning frameworks, test-time adaptation, and frequency-domain disentanglement [22], but systematic benchmarking across all three biometric modalities under a standardised cross-domain protocol has yet to be published.

Comparative Analysis of Deep Learning Paradigms: Ensemble, Transfer, and Adversarial Learning: Three deep learning paradigms appear frequently across the reviewed literature, and their relative merits deserve explicit discussion. Ensemble methods (e.g., [28, 35, 52, 59]) aggregate predictions from multiple models, which improves robustness to intra-class variation and reduces variance; their principal limitation is multiplicative inference cost, making real-time deployment on resource-constrained devices challenging. Transfer learning (e.g., [44, 53]) exploits ImageNet-pretrained weights to compensate for small biometric datasets, often yielding strong accuracy with fewer training samples; however, the domain gap between natural images and biometric captures can introduce suboptimal feature biases, particularly in texture-sensitive tasks such as fingerprint liveness detection. Adversarial learning approaches (e.g., [36, 31]) explicitly model the generative process of spoofing to produce domain-invariant representations; while theoretically appealing, they require careful hyper-parameter tuning and can suffer from training instability. In practice, the choice of paradigm should be driven by the deployment constraints: transfer learning is preferable when data is scarce and inference hardware is capable; lightweight architectures should be favoured for edge or mobile deployment; and domain-adversarial training should be considered when cross-sensor generalisation is a primary requirement.

Explainable AI in Biometric Anti-Spoofing: Although explainability is mentioned as a future direction in several reviewed papers, its practical implementation in biometric security systems raises non-trivial challenges that warrant dedicated discussion. Post-hoc explanation methods such as Grad-CAM and SHAP can highlight which spatial regions influenced a liveness decision, but they are susceptible to adversarial manipulation—an attacker aware of the explanation method could craft spoof samples that produce misleading attribution maps. Intrinsically interpretable models, by contrast, sacrifice discriminative capacity for transparency. For operational security contexts, a further complication is that auditors and security analysts require explanations at the decision

level (e.g., "this sample was rejected because of abnormal spectral texture in the periocular region"), not merely at the pixel level. Addressing these challenges requires co-design of explanation frameworks with the anti-spoofing model architecture, rather than bolting on post-hoc methods after training.

Computational Cost and Deployment Considerations: A notable gap in the surveyed literature is the near-universal omission of computational benchmarks. With few exceptions, papers report accuracy metrics without disclosing model size (parameter count), inference latency (milliseconds per frame on representative hardware), memory footprint, or energy consumption. This omission is consequential for real-world deployment: many biometric systems operate on embedded processors, smart-card readers, or edge-AI accelerators with strict timing budgets. Lightweight convolutional models and knowledge-distilled variants of large architectures are beginning to appear in the face PAD literature, but remain largely absent from fingerprint and iris PAD research. We call on future authors to report FLOPs, latency on at least one embedded or mobile platform (e.g., Raspberry Pi 4, Qualcomm Snapdragon), and the corresponding accuracy-efficiency trade-off alongside standard benchmark results.

Fingerprint and iris modalities face additional challenges due to limited public datasets and a scarcity of presentation attack samples compared to face databases. Synthetic data generation methods, such as generative adversarial networks (GANs)[50] and diffusion models[51], can address the data shortages but there is still much to be determined in terms of how realistic synthetic data must be versus how diverse it must be. Future research directions include: (i) multimodal authentication that utilizes face, iris, fingerprint cues; (ii) lightweight presentation attack detection models for edge deployment on IoT and mobile devices; (iii) explainable AI techniques to make the decision making process of these systems interpretable for security analysts; (iv) continual learning frameworks that allow detection systems to adapt to novel attack types without requiring full model retraining.

3.2 Literature Review Summary

Table 5 summarizes the key works evaluated in this survey, organized by biometric modality, and includes the method employed, core contribution, provided datasets, or performance highlights. As seen in the table, there has been a significant trend in recent years towards deep learning architectures, such as Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs), across all three modalities. Furthermore, the literature identifies a continuing challenge: while researchers achieve very high accuracy rates on certain benchmark datasets, generalizing these results across multiple hardware sensors and cross-domain contexts remains a major barrier for future research.

Table 5. Summary of reviewed image spoofing detection literature organized by biometric modality.

Ref.	Authors	Year	Modality	Method / Technique	Key Contribution	Dataset / Key Result
FACE SPOOFING DETECTION						
[16]	Banerjee et al.	2014	Face	Vulnerability Analysis	Identified key face biometric vulnerabilities and countermeasures against presentation attacks.	CVPRW 2014; Survey
[17]	Liu et al.	2024	Face	CFPL-FAS (CLIP-based VLM)	Class-free prompt learning leveraging CLIP textual features to dynamically adjust classifier weights for generalizable FAS.	Multiple benchmarks; SOTA generalization
[18]	Cao et al.	2024	Face (3D)	Flow-Attention Spatio-Temporal Network	Aggregated spatio-temporal features using optical flow attention for robust 3D mask detection.	NeurIPS 2024; 3D mask DB
[19]	Zuama et al.	2025	Face	FaceNet + Tuned DenseNet201	Feature fusion of FaceNet embeddings and fine-tuned DenseNet201 for high-performance spoofing detection.	JFAIT 2025; >98% accuracy
[20]	Chingovska et al.	2014	Face	Evaluation under spoofing attacks	Systematic evaluation framework for biometric systems under multiple spoofing attack categories.	TIFS 2014; Benchmark

[21]	Li et al.	2024	Face	Cross-Stage Relation Enhancement	Enhanced spoof material perception through cross-stage feature relations in a CNN pipeline.	Neural Networks 2024; CASIA
[22]	Zheng et al.	2024	Face	MFAE – Masked Frequency Autoencoders	Domain generalization FAS using masked frequency autoencoders to learn frequency-agnostic representations.	TIFS 2024; Multi-domain
[23]	He et al.	2015	Face	PReLU / Rectifiers (deep CNN)	Proposed parametric rectified linear units improving very deep CNN training; applied to face image classification.	ImageNet; surpassed human-level
[24]	Agarwal et al.	2016	Face	Haralick Texture + RDWT	Extracted Haralick texture features from redundant discrete wavelet transform for video replay attack detection.	BTAS 2016; Replay-Attack DB
[25]	Patel et al.	2016	Face	Eye blink + Deep Texture Features	Combined liveness cue (blink detection) with deep texture for robust 2D face spoof detection.	TIFS; Multiple public DBs
[26]	Sepas-Moghaddam et al.	2018	Face	Light Field Imaging Framework	Exploited directional light field color and texture for anti-spoofing.	IET Biometrics 2018; IST LLFFSD Database
[27]	Wang et al.	2023	Face	Consistency Regularization (CR-FAS)	Dense similarity targets enforce feature-level consistency, effective in supervised and semi-supervised settings.	TIFS 2023; CASIA-SURF, RA
[28]	Solomon &	2023	Face	FASS – Random Forest + Deep	Combined seven no-reference image quality	Electronics 2023;

	Cios			Learning	metrics with a deep classifier via random forest ensemble.	NUAA, Replay
[29]	Shijie et al.	2022	Face	Metasurface Hyperspectral Sensor	Snapshot hyperspectral imaging via metasurface nanostructures captures fine spectral cues beyond RGB.	Optica 2022; Custom DB
[30]	Liu et al.	2023	Face	Spoof Trace Disentanglement	Adversarial learning separates spoof traces from real faces in additive and inpainting phases enabling data augmentation.	TPAMI 2023; Improved long-tail
[31]	Sun et al.	2023	Face	SA-FAS – IRM-based Alignment	Aligns live-to-spoof trajectory across domains via invariant risk minimization for domain generalization.	CVPR 2023; DG benchmarks
[32]	Wang et al.	2023	Face (Forgery)	AltFreezing – 3D ConvNet	Alternating-freezing training balances temporal and spatial cues for video face forgery detection.	CVPR 2023; FF++, Celeb-DF
[33]	Turhal et al.	2024	Face	Multi-color Multi-level LBP	Device-independent multi-level LBP features in multiple color spaces for face presentation attack detection.	Vis Comput 2024; MSU-MFSD
[34]	Asmitha et al.	2024	Face	RetinaFace + I-AF algorithm	Combined RetinaFace detection with I-AF recognition prioritizing Extended Euclidean distance for anti-spoofing.	Multimed. Tools 2024; Custom
[35]	Sabri et al.	2024	Face	DenseNet201 + MiniVGG	Weighted deep ensemble of DenseNet201 and MiniVGG selected via	SIViP 2024; NUAA, CASIA-FASD

				Ensemble	comparative study of five architectures.	
[36]	Kim & Kwon	2025	Face	RGB-D + Domain Adversarial Learning	Cross-domain FAS using depth+RGB fusion; domain adversarial training.	Electronics 14(11):2182
[37]	Li et al.	2025	Face	ECA + ICD Framework	Enhanced Channel Attention + Intra-Class Differentiator to separate overlapping live/spoof distributions.	J. Imaging 11(4):116
[38]	El-Rashidy et al.	2025	Face	CCP + MTCNN	Novel Comprehensive Correlational Pattern texture descriptor for FAS.	Int. J. Mach. Learn. Cyber. 16:5295
[42]	Manjani et al.	2017	Face (3D)	Deep Dictionary Learning on SMAD	Established silicon face mask database (SMAD); multi-level deep dictionary learning for mask PAD.	TIFS 2017; SMAD DB
[44]	Lucena et al.	2017	Face (3D)	FAS-Net – VGG-16 Transfer Learning	Transfer learning from pre-trained VGG-16 for photo, video, and 3D mask presentation attack detection.	ICIAR 2017; 3DMAD, Replay
[45]	Hamdan & Mokhtar	2017	Face (3D)	ART + Maximum Likelihood Classifier	Angular Radial Transformation extracts shape features from RGB; ML classifier distinguishes real/mask.	Egypt. Inf. J. 2017; Custom
[46]	Wu et al.	2023	Face (3D)	DepthFake – Structured Light Attack	Discovered attack vector against structured-light 3D face auth; spoofs 3D liveness using a single 2D photo.	IEEE S&P 2023; Commercial

FINGERPRINT SPOOFING DETECTION						
[15]	Marasco et al.	2014	Fingerprint	Survey – Anti-spoofing Schemes	Reviewed vulnerabilities and countermeasures for fingerprint recognition including artificial finger attacks.	ACM CSUR 2014; Systematic review
[47]	Dubey et al.	2016	Fingerprint	SURF + PHOG + Gabor Wavelet Fusion	Multi-cue fusion at score level from SURF, PHOG, and Gabor features for single-image liveness detection.	TIFS 2016; LivDet 2011
[48]	Tan & Ser	2010	Fingerprint	Ridge Signal + Valley Noise Analysis	Fused ridge signal quality with valley noise statistics; tested across materials and moisture levels.	Pattern Recog. 2010; EER 0.9%
[49]	Almajmaie et al.	2019	Fingerprint	Associative Memory Architecture	Modified multi-connect architecture (MMCA) for fingerprint matching; tested on FVC2004 and NIST DBs.	Cogn. Syst. Res. 2019; 99.5%
[50]	Grosz & Jain	2022	Fingerprint	SpoofGAN – Synthetic Spoof Generation	GAN-based synthesis of realistic spoof fingerprint images to augment small PAD training sets.	TIFS 2022; LivDet-2015, 2017
[51]	Tang et al.	2024	Fingerprint	WGAN-GP + DDPM + CycleWGAN-GP	High-quality fingerprint patch synthesis using diffusion models and style transfer with cycle autoencoder.	Springer 2024; FVC datasets
[52]	Cheniti et al.	2025	Fingerprint	VGG16 + ResNet50 Dual Model	Dual-stream pre-trained model; ACE 0.28% on LivDet 2013.	Sensors 25(5)

[53]	Pallakonda et al.	2025	Fingerprint	TL-Efficient-SE (EfficientNetB0 + SE)	Transfer learning + squeeze-and-excitation attention; cross-sensor generalization.	MAKE 7(4):113
IRIS SPOOFING DETECTION						
[55]	Daugman	1999	Iris	Spectrographic Ocular Tissue Analysis	Sensor-level anti-spoofing using spectral properties of ocular tissue (fat/blood) as liveness cues.	IrisCodes; Glass eye, cadaver
[56]	Raghavendra & Busch	2014	Iris	Light Field Camera PAD	Focus variance across depth images from LFC across a 104-pattern library detects presented artefacts.	IJCB 2014; Custom LFC DB
[57]	Raja et al.	2015	Iris	Eulerian Video Magnification (EVM)	Magnified pupillary oscillation from iris video as liveness cue; effective against video replay attacks.	TIFS 2015; ATVS-FIr DB
[58]	Bhuiyan & Czajka	2024	Iris	Conditional StyleGAN Iris Synthesis	Forensic iris synthesis via StyleGAN for post-mortem iris identification; expands training for cadaver irises.	WACV 2024; Custom post-mortem DB
[59]	Sharma & Selwal	2025	Iris	IensNet (DenseNet161 + ResNet + VGGNet)	Ensemble of three fine-tuned deep models for iris spoof detection.	Multimed. Tools Appl. 2025
[60]	Das et al.	2026	Iris	CNN Iris Liveness Detection	CNN on custom authentic+synthetic iris dataset; 92.51% accuracy.	NICEDT 2025/Springer 2026

4 | Conclusion

Biometric technology has greatly developed over the past few decades and is being employed extensively today for identity authentication and verification. The primary goal of this survey was to assess the practical applications of biometric systems as well as the security-related shortcomings of these systems. As biometric use becomes increasingly common, it is important that individuals and organizations be aware of the risks associated with image spoofing. To that end, this survey presented a review of the current state-of-the-art in presentation attacks, including image-based spoofing for fingerprint, iris, and facial modalities. In addition, the survey reviewed some of the most frequently used techniques across each modality, exploring their operating characteristics and generalizing capabilities.

Building upon this review, a synthesis of open research problems reveals three critical areas that stand out as requiring urgent and coordinated community effort. First, multimodal spoofing—where an adversary simultaneously attacks two or more biometric channels (e.g., face and iris in a multi-factor system)—is largely unexplored; existing detectors treat each modality independently, creating exploitable seams. Second, synthetic identity generation through generative AI (large diffusion models, face-swapping pipelines) now produces identities indistinguishable from real photographs to both human observers and standard PAD systems; new detection paradigms based on forensic frequency analysis, physiological signal detection, or source-model attribution are needed. Third, adaptive attacks driven by reinforcement-learning or gradient-based optimization against white-box PAD models represent an emerging threat class for which neither robust defenses nor standardized evaluation protocols currently exist. Addressing these problems will require open benchmarks, cross-institutional data sharing, and evaluation frameworks that report both accuracy and computational cost under realistic operating conditions. Ultimately, this survey has made it clear that no single biometric system is entirely foolproof against a determined attacker. Continued research must prioritize building more resilient and adaptable defenses to stay ahead of these ever-evolving spoofing threats.

Acknowledgments

The author gratefully acknowledges the editors and reviewers for their constructive feedback. Sincere thanks are also extended to the supervisors for their invaluable guidance, critical assessment, and rigorous review throughout this study.

Funding

This research has no funding source.

Data Availability

Data sharing is not applicable to this article, as no new datasets were generated or analyzed during this study.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

References

[1] Jain A, Ross A, and Pankanti S. Biometrics: A tool for information security. IEEE Trans. Inform. Forensics Security. vol. 1, no. 2, pp. 125–143, June 2006.

[2] Jain A K, Ross A, and Prabhakar S. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[3] Schuckers S A C. Spoofing and anti-spoofing measures. Information Security Technical Report, vol. 7, no. 4, pp. 56–62, 2002.

[4] Boulkenafet Z, Komulainen J and Hadid A. Face antispoofing based on color texture analysis. Proc. IEEE Int. Conf. on Image Processing, pp. 2636–2640, 2015.

[5] Boulkenafet Z, Komulainen J and Hadid A. Face spoofing detection using colour texture analysis. IEEE Trans. Information Forensics and Security, vol. 11, no. 8, pp. 1818–1830, 2016.

[6] Komulainen J and Zhao G. Generalized face anti-spoofing by detecting pulse from face videos. Proc. IEEE 23rd Int. Conf. on Pattern Recognition, pp. 4239–4244, 2016.

[7] Liu S Q, Lan X Y and Yuen P C. Remote photoplethysmography correspondence feature for 3D mask face presentation attack detection. Proc. European Conf. on Computer Vision, pp. 558–573, 2018.

[8] Kollreider K, Fronthaler H, and Bigun J. Evaluating liveness by face images and the structure tensor. Fourth IEEE Workshop on Automatic Identification Advanced Technologies, pp. 75–80, 2005.

[9] A. Hadid, N. Evans, S. Marcel, and J. Fierrez, "Biometrics systems under spoofing attack: An evaluation methodology and lessons learned," IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 20–30, 2015.

[10] Galton F. Finger Prints. New York, NY, USA: Macmillan, 1892.

[11] Pankanti S, Prabhakar S, and Jain A K. On the individuality of fingerprints. IEEE Trans. Pattern Anal. Mach. Intell., vol. 24, no. 8, pp. 1010–1025, Aug. 2002.

[12] Trivedi A K, Kumar K, Aggarwal R and Garg A. An Approach to Integration of Gait and Fingerprint Features for Advanced Biometric Recognition Technology. 2024 14th Int. Conf. Cloud Computing, Data Science Engineering, pp. 453–457.

[13] Hu C, Li Y, Feng Z and Wu X. Image understanding for iris biometrics: A survey. Computer Vision and Image Understanding, vol. 110, no. 2, pp. 281–307, 2008.

[14] Daugman J. How iris recognition works. Proceedings of the IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 21–30, 2004.

[15] Marasco E. A Survey on Antispoofing Schemes for Fingerprint Recognition. ACM Comput. Surv., vol. 47, no. 2, 2014.

[16] Banerjee S, Jain A, Jiang Z, Memon N, Togelius J. Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions. IEEE CVPRW, 2014.

[17] Liu A, Xue S, Gan J, Wan J, Liang Y, Deng J, Escalera S, Lei Z. CFPL-FAS: Class Free Prompt Learning for Generalizable Face Anti-spoofing. ArXiv, abs/2403.14333, 2024.

[18] Cao, Yuxin, Yian Li, Yumeng Zhu, Derui Wang, and Minhui Xue. "Flow-attention-based spatio-temporal aggregation network for 3D mask detection." Advances in Neural Information Processing Systems 36 (2023): 21920-21932.

[19] Zuama, Leygian Reyhan, Ajib Susanto, Stefanus Santosa, Hong-Seng Gan, and Arnold Adimabua Ojugo. "High-Performance Face Spoofing Detection using Feature Fusion of FaceNet and Tuned DenseNet201." Journal of Future Artificial Intelligence and Technologies 1, no. 4 (2025): 385-400.

[20] Chingovska I, Anjos A R, and Marcel S. Biometrics evaluation under spoofing attacks. IEEE Trans. Information Forensics and Security, vol. 9, no. 12, pp. 2264–2276, 2014.

[21] Li D, Chen G, Wu X, Yu Z, Tan M. Face anti-spoofing with cross-stage relation enhancement and spoof material perception. Neural Networks, vol. 175, 2024.

[22] Zheng, Tianyi, Bo Li, Shuang Wu, Ben Wan, Guodong Mu, Shice Liu, Shouhong Ding, and Jia Wang. "Mfae: Masked frequency autoencoders for domain generalization face anti-spoofing." IEEE transactions on information forensics and security 19 (2024): 4058-4069.

[23] He K, Zhang X, Ren S, Sun J. Delving deep into rectifiers: surpassing human-level performance on ImageNet classification, 2015.

[24] Agarwal A, Singh R, Vatsa M. Face anti-spoofing using Haralick features. IEEE 8th Int. Conf. Biometrics Theory, Applied Systems BTAS, 2016.

[25] K. Patel, H. Han, and A. K. Jain, "Secure Face Unlock: Spoof Detection on Smartphones," IEEE Transactions on Information Forensics and Security, vol. 11, no. 10, pp. 2268-2283, Oct. 2016.

[26] Sepas-Moghaddam, A., Malhadas, L., Correia, P. L., & Pereira, F. (2018). Face spoofing detection using a light field imaging framework. IET Biometrics, 7(1), 39-48.

[27] Wang, Zezheng, Zitong Yu, Xun Wang, Yunxiao Qin, Jiahong Li, Chenxu Zhao, Xin Liu, and Zhen Lei. "Consistency regularization for deep face anti-spoofing." IEEE Transactions on Information Forensics and Security 18 (2023): 1127-1140.

[28] Solomon E, Cios K J. FASS: Face Anti-Spoofing System Using Image Quality Features and Deep Learning. Electronics, 12, 2199, 2023.

[29] Shijie Rao, Yidong Huang, Kaiyu Cui, and Yali Li. Spoofing face recognition using a metasurface-based snapshot hyperspectral image sensor. Optica, 9, 1253–1259, 2022.

[30] Liu Y and Liu X. Spoof Trace Disentanglement for Generic Face Anti-Spoofing. IEEE Trans. PAMI, vol. 45, no. 3, pp. 3813–3830, 2023.

[31] Sun Y, Liu Y, Liu X, Li Y and Chu W. Rethinking Domain Generalization for Face Anti-spoofing: Separability and Alignment. IEEE/CVF CVPR, Vancouver, 2023, pp. 24563–24574.

[32] Wang Z, Bao J, Zhou W, Wang W and Li H. AltFreezing for More General Video Face Forgery Detection. IEEE/CVF CVPR, Vancouver, 2023, pp. 4129–4138.

[33] Turhal U, Gunay Yilmaz A, Nabiyev V. A new face presentation attack detection method based on face-weighted multi-color multi-level texture features. Vis Comput, 40, 1537–1552, 2024.

[34] Asmitha P, Rupa Ch, Nikitha S, Hemalatha J, Sahu A K. Improved multiview biometric object detection for anti spoofing frauds. Multimedia Tools and Applications, 2024.

[35] Sabri M A, Ennouni A, Aarab A. An effective facial spoofing detection approach based on weighted deep ensemble learning. SIViP, 18, 935–942, 2024.

[36] Kim, Hee-jin, and Soon-kak Kwon. "Anti-Spoofing Method by RGB-D Deep Learning for Robust to Various Domain Shifts." Electronics 14, no. 11 (2025): 2182.

[37] Li, Ye, Wenzhe Sun, Zuhe Li, and Xiang Guo. "Face anti-spoofing based on adaptive channel enhancement and intra-class constraint." Journal of imaging 11, no. 4 (2025): 116.

[38] El-Rashidy, Mohamed A., Amira E. Enab, Salah S. Elagooz, Nawal A. El-Fishawy, and Marwa Radad. "A novel texture descriptor using machine learning for face anti-spoofing detection." International Journal of Machine Learning and Cybernetics 16, no. 7 (2025): 5295-5316.

[39] Galbally J, and Satta R. Three-dimensional and two-and-a-half-dimensional face recognition spoofing using three-dimensional printed models. IET Biometrics, vol. 5, no. 2, pp. 83–91, 2015.

[40] Pan G, Sun L, Wu Z, and Lao S. Eyeblink-based anti-spoofing in face recognition from a generic web camera. 11th IEEE Int. Conf. Computer Vision, pp. 1–8, 2007.

[41] Feng, Litong, Lai-Man Po, Yuming Li, Xuyuan Xu, Fang Yuan, Terence Chun-Ho Cheung, and Kwok-Wai Cheung. "Integration of image quality and motion cues for face anti-spoofing: A neural network approach." Journal of Visual Communication and Image Representation 38 (2016): 451-460

[42] Manjani I, Tariyal S, Vatsa M, Singh R, Majumdar A. Detecting silicone mask-based presentation attack via deep dictionary learning. IEEE Trans. Inf. Forensics Secur., 12(7), 1713–1723, 2017.

[43] Menotti, David, Giovani Chiachia, Allan Pinto, William Robson Schwartz, Helio Pedrini, Alexandre Xavier Falcao, and Anderson Rocha. "Deep representations for iris, face, and fingerprint spoofing detection." IEEE Transactions on Information Forensics and Security 10, no. 4 (2015): 864-879.

[44] Lucena O, Junior A, Moia V, Souza R, Valle E, Lotufo R. Transfer learning using convolutional neural networks for face anti-spoofing. Int. Conf. Image Analysis and Recognition, Springer, 2017, pp. 27–34.

[45] Hamdan B, Mokhtar K. The detection of spoofing by 3D mask in a 2D identity recognition system. Egypt. Inf. J., 2017.

[46] Wu Z, Cheng Y, Yang J, Ji X and Xu W. DepthFake: Spoofing 3D Face Authentication with a 2D Photo. IEEE Symposium on Security and Privacy (SP), San Francisco, 2023, pp. 917–933.

[47] Dubey R K, Goh J, and Thing V L L. Fingerprint Liveness Detection From Single Image Using Low-Level Features and Shape Analysis. IEEE Trans. Inf. Forensics Secur., vol. 11, no. 7, pp. 1461–1475, 2016.

[48] Tan B and Ser S A. Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise. Pattern Recognition, vol. 43, no. 8, pp. 2845–2857, 2010.

[49] Almajmaie L, Ucan O N, and Bayat O. Fingerprint recognition system based on modified multi-connect architecture (MMCA). Cogn. Syst. Res., vol. 58, pp. 107–113, 2019.

[50] Grosz S A and Jain A K. SpoofGAN: Synthetic Fingerprint Spoof Images. IEEE Trans. Inf. Forensics Security, 18, 730–743, 2022.

[51] Tang, Weizhong, Diego Figueroa, Donglin Liu, Kerstin Johnsson, and Alexandros Sopasakis. "Enhancing fingerprint image synthesis with GANs, diffusion models, and style transfer techniques." arXiv preprint arXiv:2403.13916 (2024).

[52] Cheniti, Mohamed, Zahid Akhtar, and Praveen Kumar Chandaliya. "Dual-model synergy for fingerprint spoof detection using vgg16 and resnet50." Journal of Imaging 11, no. 2 (2025): 42.

[53] Pallakonda, Archana, Rayappa David Amar Raj, Rama Muni Reddy Yanamala, Christian Napoli, and Cristian Randieri. "TL-Efficient-SE: A Transfer Learning-Based Attention-Enhanced Model for Fingerprint Liveness Detection Across Multi-Sensor Spoof Attacks." Machine Learning and Knowledge Extraction 7, no. 4 (2025): 113.

[54] Daugman J. High confidence visual recognition of persons by a test of statistical independence. IEEE TPAMI, vol. 15, pp. 1148–1161, 1993.

[55] Daugman J. Biometrics: Personal Identification in a Networked Society — Recognizing Persons by their Iris Patterns. pp. 103–121, Kluwer Academic Publishers, 1999.

[56] Raghavendra R and Busch C. Presentation attack detection on visible spectrum iris recognition by exploring inherent characteristics of light field camera. Proc. IEEE IJCB, 2014.

[57] Raja, Kiran B., Ramachandra Raghavendra, and Christoph Busch. "Video presentation attack detection in visible spectrum iris recognition using magnified phase information." IEEE Transactions on Information Forensics and Security 10, no. 10 (2015):

2048-2056.

[58] Bhuiyan, Rasel Ahmed, and Adam Czajka. Forensic Iris Image Synthesis. Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision. 2024.

[59] Sharma, Deepika, and Arvind Selwal. "IensNet: A novel and efficient approach for iris spoof detection via ensemble of deep models." Multimedia Tools and Applications 84, no. 27 (2025): 33237-33266.

[60] Das, Niladri, Poulomi Deb, Swanirbhar Majumder, and Priyanka Debnath. "Liveness Detection in Iris Using CNN Model." In NIELIT's International Conference on Communication, Electronics and Digital Technologies, pp. 355-364. Singapore: Springer Nature Singapore, 2025.